

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Applicant: COHEN	§	
	§	
Serial No.: 10/826,503	§	
	§	
Filed: April 19, 2004	§	Group Art Unit: 2134
	§	
For: METHOD FOR PREVENTING	§	Attorney
ACTIVATION OF	§	Docket: 2808/28
MALICIOUS OBJECTS	§	
	§	
Examiner: Jacob Lipman	§	

TRANSMITTAL OF APPEAL BRIEF

Commissioner of Patents and Trademarks
Alexandria, Virginia 22313

Dear Sir:

Transmitted herewith in triplicate is the APPEAL BRIEF in this application with respect to the Notice of Appeal filed on Sep. 5, 2007.

The application is on behalf of small entity.

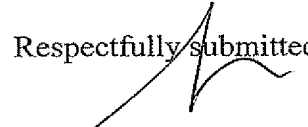
Pursuant to 37 CFR 1.17(f) the fee for filing the Appeal Brief is \$ 255

Please charge Account No. 06-2140 the sum of \$ 255. A duplicate copy of this transmittal letter is attached.

If any additional extension and/or fee is required, this is a request therefor and to charge Account No. 06-2140.

If any additional fee for claims is required, please charge Account No. 06-2140.

Respectfully submitted,



Mark M. Friedman
Attorney for Applicant
Registration No. 33,883

Date: October 25, 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Applicant: COHEN	§	
	§	
Serial No.: 10/826,503	§	
	§	
Filed: April 19, 2004	§	Group Art Unit: 2134
	§	
For: METHOD FOR PREVENTING	§	Attorney
ACTIVATION OF	§	Docket: 2808/28
MALICIOUS OBJECTS	§	
	§	
Examiner: Jacob Lipman	§	

Commissioner of Patents and Trademarks
Alexandria, Virginia 22313
ATTENTION: Board of Patent Appeals and Interferences

APPELLANT'S BRIEF

Dear Sir:

This is in furtherance of the Notice of Appeal filed in this case on Sep. 5, 2007.

The fees required under § 1.17(f) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate.

This brief contains these items under the following headings and in the order set forth below:

- I. REAL PARTY IN INTEREST
- II. RELATED APPEALS AND INTERFERENCES
- III. STATUS OF CLAIMS
- IV. STATUS OF AMENDMENTS
- V. SUMMARY OF CLAIMED SUBJECT MATTER

- VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
- VII. ARGUMENTS - REJECTION UNDER 35 USC §103(a)
- VIII. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL
- IX. APPENDIX OF EVIDENCE
- X. APPENDIX OF RELATED PROCEEDINGS

I. REAL PARTY IN INTEREST

Aladdin Knowledge Systems, Inc, is the real party in interest, and is the assignee of Application No. 10/826,503.

II. RELATED APPEALS AND INTERFERENCES

The Appellant's legal representative, or assignee, does not know of any other appeal or interferences which will affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

The subject patent application was originally filed with 11 claims. During the course of prosecution, Claim 3 was cancelled. Claims 1, 2, and 4-11 are presently pending in the application, and all stand rejected.

A Notice of Appeal was filed on Sep. 5, 2007, appealing the Office Action mailed April 9, 2007, finally rejecting Claims 1, 2, and 4-11.

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 2, and 4-11

B. STATUS OF ALL THE CLAIMS

1. Claims cancelled: 3
2. Claims withdrawn from consideration but not cancelled: none
3. Claims pending: 1, 2, and 4-11
4. Claims allowed: none
5. Claims rejected: 1, 2, and 4-11

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 2, and 4-11

IV. STATUS OF AMENDMENTS

One amendment was filed in response to the Final Office Action mailed April 9, 2007, canceling claim 3. In the Advisory Action Before Appeal mailed June 13, 2007, this proposed amendment was entered for purposes of appeal.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The subject matter of the presently-pending claims is directed to a method for protecting a computer from attack by malicious executable data objects that may be sent to that computer via a data communications network, in such a way that minimizes the transmission delay in delivering data objects to the computer.

At a checkpoint through which data objects pass on their way to the computer, a data object is enclosed within an envelope file created at the checkpoint to contain that specific data object — it is this envelope file containing the data object, rather than the data object itself, which is thereafter sent to the computer. The envelope file is executable, having code for extracting the data object contained therein, and also has an integrity indicator to show whether the contained data object is benign or malicious.

During the time period over which an envelope file is transmitted from the checkpoint to the computer over the network (one data packet at a time), the data object that was placed in the envelope is inspected at the checkpoint to determine if that data object is benign or malicious. If the data object is benign, the integrity indicator of the envelope file containing the data object is marked as “benign”. Then the transmission to the computer is completed, whereupon the data object may be extracted from the envelope file by using the extraction code therein. If, however, the data object is malicious, then the integrity indicator is marked as “malicious” so that other appropriate action may be taken — such as deleting the data object, alerting the user to the malicious content, and so forth.

In addition to the use of an envelope file to enclose and isolate potentially malicious data objects, the presently-pending claims stipulate that at least one part of the envelope file be withheld at the checkpoint until the inspection process is

complete and a determination of the contained data object is made. In this manner, the bulk of the envelope file containing the data object can be sent to the computer without waiting for the inspection to complete, thereby minimizing the transmission delay. At the same time, however, withholding a part of the envelope file guarantees that in the case of a malicious contained data object, no portion of the malicious data object can be activated at the computer, because a complete envelope file is necessary before extraction of the contained data object can be performed. The transmission delay is minimal because only the withheld part of the envelope file need be transmitted to the computer upon completion of the inspection, and this part may be as small as a single data packet.

In the above manner, the present invention provides a method for preventing the activation of malicious data objects at the computer while minimizing transmission delays.

The key features above are recited as limitations in independent claim 1 of the present application, and all remaining presently-pending claims depend from claim 1.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

In a final Office Action mailed April 9, 2007 (herein “the Office Action”), the Examiner rejected the presently-pending claims under 35 USC §103(a) as being unpatentable over US Patent Number 6,088,803 to Tso, et al., in view of US Patent Publication Number 2004/0054928 of Hall.

Tso discloses a system for inspecting a data object that is being sent to a computer over a data network, in which a part of the data object is withheld pending the completion of the inspection process.

Tso fails to disclose an envelope file containing the data object, which is recited as a limitation in presently-pending independent claim 1; moreover Tso fails to disclose an integrity indicator, which is part of the envelope file. Because this executable code and the integrity indicators are limitations recited in presently-pending claim 1, Tso thus fails to meet all the limitations of the present claims. The Examiner, however, has construed Tso’s data object without the withheld part to be an envelope file (Office Action page 3 line 11).

Despite construing Tso’s data object without the withheld part as an envelope file, however, the Examiner does take note of the fact that Tso fails to disclose the inclusion of executable code which extracts the object (Office Action page 3 lines 11-12).

The Examiner then cites Hall as using an “executable wrapper” to protect files, stating that “Hall discloses an executable wrapper used to protect files”, and that “Hall teaches that the wrapper protects a file from being executed without checking an authorization algorithm by hiding the object, and supplementing an executable wrapper that will release the object if authorization is checked” (Office Action page 3

lines 12-16, Hall paragraphs [0044]-[0045]). This is the basis for the current 35 USC §103(a) rejection of the claims as obvious over Tso in view of Hall.

VII. ARGUMENTS - REJECTION UNDER 35 USC §103(a)

In a Response to the Office Action, filed June 6, 2007 (herein “the Response”, which is hereby incorporated by reference into the present Appellant’s Brief), the Applicants respectfully traverse the Office Action’s 35 USC §103(a) rejection on the grounds that, to a person having ordinary skill in the art, it is technically not possible to combine Tso and Hall in a manner that achieves the structural limitations recited in presently-pending claim 1.

Specifically, Hall fails to disclose any material related to the structural limitations of the presently-pending claims or capable of being combined with Tso or to modify Tso to achieve those limitations. For example, Hall fails to teach or reasonably suggest executable code that extracts a data object from an envelope file.

Hall is directed to a method for preventing unauthorized personnel from executing fully-installed software (such as operating system commands) within a computer system. Hall teaches relocating those system commands from their standard locations to hidden locations, and substituting proxy executables (which Hall refers to as “wrappers”) in place thereof in the standard locations. These “wrappers” (proxy executables) have the same name as the original system commands, but contain only code for checking user authorization and conditionally executing the relocated original system command software. Thus, when a user tries to execute one of the protected system commands, he or she will instead be executing the “wrapper” (a proxy). The “wrapper” proxy then checks the user’s authorization status, and only if that user is permitted to access the desired system command is that system command actually executed by the “wrapper” proxy. It is emphasized Hall fails to teach or reasonably suggest that a “wrapper” contains or comprises the system command software.

Combining Tso with Hall does not teach or reasonably suggest all the limitations of presently-pending independent claim 1. Hall's "wrappers" are structurally completely different from the envelope files of the present claims. A "wrapper" according to Hall does not contain or comprise another data object, as does the envelope file of the present claims. Moreover, a "wrapper" according to Hall does not contain or comprise code for extracting the data object, nor an integrity indicator for the data object.

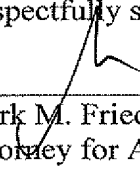
Tso and Hall, individually as well as combined, fail to teach or reasonably suggest putting a data object passing through a checkpoint into an executable envelope file having code for extracting that data object, as recited in presently-pending independent claim 1. Moreover, the combination of Tso and Hall does not have a reasonable expectation of success in meeting the limitations recited in the presently-pending claims.

In an Advisory Action mailed June 13, 2007 (herein "the Advisory Action"), the Examiner claims that "Applicant argues that combining Tso and Hall would not have been obvious to one of ordinary skill in the art since Tso is protecting from malicious code to be installed, and Hall is protected from unauthorized execution." The Applicants respectfully disagree with this characterization of their argument, in that the Applicants' principal position (as clearly put forth in the Response) is that it is technically *not possible* to combine Tso and Hall in a manner that meets the limitations of the presently-pending claims; and therefore Tso in view of Hall fails to teach or reasonably suggest all the claim limitations; and further that Tso in view of Hall as proposed in the Office Action fails to have a reasonable expectation of success. Both meeting all claim limitations and a reasonable expectation of success are stipulated *inter alia* in MPEP 2143 as necessary for a *prima facie* case of

obviousness under 35 USC §103(a). The Applicants continue to maintain that, absent these two necessary elements, Tso in view of Hall as proposed in the Office Action fails to sustain a 35 USC §103(a) rejection.

The Applicants further note that in both the Office Action and the Advisory Action, the Examiner acknowledges that Tso and Hall protect against different types of attacks against the computer, and proposes that there is a motivation to combine Tso and Hall in order to protect against different types of attack. The Applicants respectfully maintain that this proposed motivation is irrelevant to the present case, because whether or not Tso and Hall can be employed simultaneously or sequentially in a computer environment to protect against different attacks is irrelevant to the present case; simultaneous or sequential application of two different methods is not the same as *combining* those methods, or *modifying* one method with the other. What is relevant to the present case is that Tso and Hall *cannot be combined*, and that Tso *cannot be modified* by Hall to achieve the structural limitations of the present independent claim 1, nor is there any reasonable expectation of success in attempting to combine them or to use one to modify the other.

Respectfully submitted,



Mark M. Friedman
Attorney for Applicant
Registration No. 33,883

Date: October 25, 2007

VIII. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

The text of the claims on appeal is:

1. A method for preventing activating a malicious object passing through a checkpoint, and decreasing the overall inspection delay thereof, the method comprising the steps of:

- a. at said checkpoint, creating an envelope file, being an executable file comprising: said object; code for extracting said object from said envelope file; and an indicator for indicating the integrity of said object;
- b. forwarding said envelope file instead of said object toward its destination, while holding at least a part of said envelope file which comprises said indicator;
- c. inspecting said object;
- d. setting said indicator on said envelope file to indicate the inspection result thereof, and
- e. releasing the rest of said envelope file.

2. A method according to claim 1, wherein said checkpoint is selected from a group comprising: a gateway server, a proxy server.

3. (Canceled)

4. A method according to claim 1, wherein the name of said envelope file is identical to the name of the inspected object.

5. A method according to claim 1, wherein the name of said envelope file differs than the name of the inspected object.

6. A method according to claim 1, wherein said indicator is selected from a group comprising: a CRC of at least one part of said envelope file, a CRC of at least one part of said inspected object, a checksum of at least one part of said envelope file,

a checksum of at least one part of said inspected object, a value stored within said envelope file, absence of a part of said envelope file, absence of a part of said object.

7. A method according to claim 1, wherein at least a part of said object is secured.

8. A method according to claim 1, wherein at least a part of said envelope file is secured.

9. A method according to claim 1, wherein said indicator is stored within the last part of said envelope file.

10. A method according to claim 1, wherein said envelope file further comprises code for displaying an acknowledgment.

11. A method according to claim 10, wherein said acknowledgment indicates integrity of said object.

IX. APPENDIX OF EVIDENCE

NONE

X. APPENDIX OF RELATED PROCEEDINGS

NONE